(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2004 (15.01.2004)

PCT

(10) International Publication Number
WO 2004/006074 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/IB2003/003120

(22) International Filing Date: 7 July 2003 (07.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02291728.0 9 July 2002 (09.07.2002) EP

(71) Applicant *(for all designated States except US)*: **SCHLUMBERGER SYSTEMES** [FR/FR]; 50, avenue Jean Jaurès, F-92120 Montrouge (FR).

(71) Applicant *(for MC only)*: **SCHLUMBERGER MALCO, INC** [US/US]; 9800 Reistertown, Owing Mills, MD 21117 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **AKKAR, Mehdi-Laurent** [FR/FR]; 17 rue Lafouge, F-94250 Gentilly (FR). **GOUBIN, Louis** [FR/FR]; 4 rue Mizon, F-75015 Paris (FR).

(74) Common Representative: **SCHLUMBERGER SYSTEMES**; c/o Patricia Renault, Intellectual Property Department/Direction, Propriété Intellectuelle, 36-38, rue de la Princesse BP 45, F-78431 Louveciennes Cedex (FR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

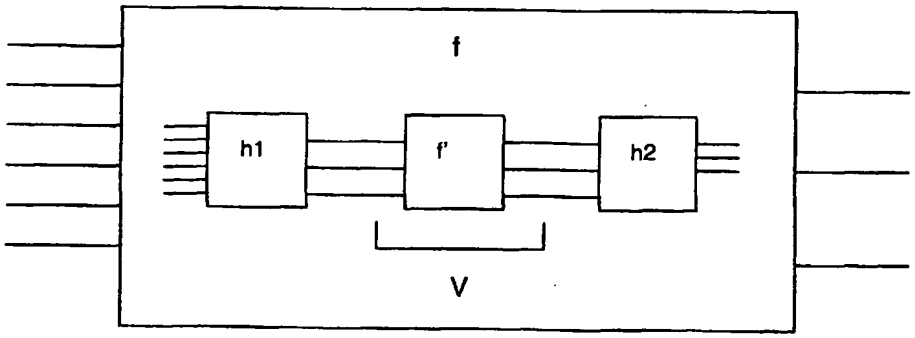
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD TO SECURE AN ELECTRONIC ASSEMBLY AGAINST ATTACKS BY ERROR INTRODUCTION



(57) Abstract: The invention concerns a method to secure an electronic assembly implementing any algorithm against attacks by error introduction. The method according to the invention consists in performing an additional calculation using a verification function on at least one intermediate result in order to obtain a calculation signature and in performing a least once more all or part of the calculation in order to recalculate said signature and compare them in order to detect a possible error.

WO 2004/006074 A2